PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

Case Management System (CMS)

DoD Component Name:

Defense Finance and Accounting Service (DFAS)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel * and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ **New DoD Information System** ☐ **New Electronic Collection**

☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR** Enter DITPR System Identification Number 8679

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** **Enter UPI** 007-97-01-20-02-1878-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

☐ **No**

d. Does the DoD information system or electronic collection have a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** **Enter Privacy Act SORN Identifier** T7340b

DoD Component-assigned designator, not the Federal Register number. Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at:
http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

☐ **No**

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations; 37 U.S.C. Chapters 1-19; DoD Financial Management Regulations 7000.14-R; and E.O. 9397(SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

CMS is a management tool system used for tracking, resolving and reporting on military pay and personnel related cases. It provides a single source of information for monitoring military pay problems in a timely and efficient manner, to include providing visibility to appropriate levels of management, permitting feedback to service members, and facilitating the identification of problem trends.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that CMS, with its collection of PII, could be compromised. All systems are also vulnerable to insider threats. These privacy risks have been mitigated through physical, technical, and administrative safeguards that meet standards established by the Department of Defense (DoD) and the National Institute of Standards and Technology (NIST). Access to the facilities is restricted to authorized DoD employees and contractors. Managed firewalls prevent access by other systems or network traffic not specifically identified in the firewall rule base. Access controls limit access to the application and/or specific functional areas of the application. Individuals are granted access to the system only after they have been verified to have a defined need to access the information and have gone through background and employment investigations. Additionally, users are given only those system privileges that are necessary for their job requirements. A security Certification and Accreditation (C&A) for the system was completed in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA). The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years, and is also reviewed at least annually to maintain currency. DFAS adheres to physical protections of PII as described in accordance with DFAS 5200.1-R. IA Policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data, to include PII, for all DFAS systems. Management responsibilities for protecting data are maintained in DFAS 8500.1.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.** Specify

PII will be shared with internal DFAS organizations that demonstrate a 'need to know' (e.g., military pay support).

☒ **Other DoD Components.** Specify

PII is shared with the Department of the Army (e.g. personnel offices).

☐ **Other Federal Agencies.** Specify

☐ **State and Local Agencies.** Specify

☐ **Contractor** (enter name and describe the language in the contract that safeguards PII.) Specify

☐ **Other** (e.g., commercial providers, colleges). Specify

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

PII is provided electronically to CMS through interfaces with the following DFAS systems: DJMS- AC (Active Component), DJMS-RC (Reserve Component), and MyPay. Case Management System (CMS) does NOT collect PII directly from the individual.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

PII is provided electronically to CMS through interfaces with the following DFAS systems: DJMS-AC (Active Component), DJMS-RC (Reserve Component), and MyPay. Case Management System (CMS) does NOT collect PII directly from the individual.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement**

☐ **Privacy Advisory**

☐ **Other**

☐ **None**

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.